

1 beforehand. And, when both match, the phone is connected to
2 the remote phone number, thereby the communication time is
3 calculated for accounting. In case the identification
4 information and the phone number are stolen and set in
5 another portable telephone and the telephone is used, the
6 accounting is done on the basis of the identification
7 information, thereby the normal owner of the telephone comes
8 to suffer the damage. Especially, because such portable
9 telephones use a radio wave so as to send both phone number
10 and identification information respectively, those
11 information items are easily stolen; even when those items
12 are encrypted, they are always exposed to a peril of being
13 decrypted and used illegally.

14 Consequently, the identification number of each portable
15 telephone is devised so as not to be stolen and the user is
16 permitted to have only one portable telephone having an
17 identification number and a phone number corresponding to
18 the identification number under one contraction. Published
19 Unexamined Patent Application No. 8-340579 discloses such a
20 technique that prevents a portable telephone from a
21 fraudulent use. In the case of a conventional portable
22 telephone, the subscriber's number, mobile station number,
23 and identification information including both certification
24 and secret key are scrambled by a scramble code and the
25 scrambled identification information is stored in the
26 non-volatile RAM of the control section of the telephone,
27 which includes a CPU. And, the initial value of the
28 scramble code is stored in the ROM of the control section
29 and the control section is provided with an algorithm that
30 generates the scramble code. In addition, because the
31 initial value of such the scramble code is common to every

1 product, it is easy to copy the content and the algorithm
2 stored in the control section into the control section of
3 another portable telephone, to substantially steal the
4 portable telephone of any person. Consequently, according
5 to the invention disclosed in the above specification, the
6 initial value of a scramble code is set differently in each
7 portable telephone and the identification information is
8 scrambled when it is written in its EEPROM. The
9 identification information is descrambled to be sent when a
10 call is to be made from the telephone.

11 Published Unexamined Patent Application No. 6-291835
12 discloses another invention for preventing a portable
13 telephone from being used by any person other than the true
14 owner without the owner's permission when the portable
15 telephone is left behind, stolen, etc. According to this
16 invention, a portable telephone, when its phone number is
17 registered, is connected to a number registration device in
18 which the personal identification number (PIN) code is
19 stored. Then, the user (owner) inputs the PIN code with use
20 of input keys. The phone number is registered in the phone
21 number memory of the portable telephone via a connection
22 terminal only when the inputted PIN code agrees to the code
23 stored in the PIN code memory. And, to use the registered
24 phone number, the user is requested to input the select code
25 of the registered phone number with use of a select key of
26 the portable telephone. Because the portable telephone is
27 enabled to send data only via the registered phone number,
28 the telephone can be prevented from being used without the
29 owner's permission.

30 And, Published Unexamined Patent Application No. 4-310026

1 discloses still another technique for preventing an
2 identification number specific to a communication device
3 from being read and used intentionally. According to this
4 technique, such a specific identification number is
5 converted in a predetermined procedure so as to be stored
6 together with an error correction code, thereby preventing
7 the identification number from an illegal use. In addition,
8 when the identification number is read, the data error is
9 corrected and it is converted to the original specific
10 identification number. In case an error correction is
11 further done for the identification number, therefore, the
12 corrected data is stored in the storage, thereby data
13 damages are prevented.

14 Published Unexamined Patent Application No. 11-146057
15 discloses a system that can identify the user of a mobile
16 telephone without requesting the user to input his/her
17 password so as to prevent a fraudulent use of the telephone.
18 According to this invention, which is a technique that
19 prevents an illegal use of a stolen or lost portable
20 telephone with fraudulent use of the password, the inventor
21 et al have directed their attention to the inconvenience
22 that the user must learn and input a password and employs
23 such user's physical features as voice, carbon dioxide
24 density at a breathing time, finger print, etc. as an
25 identifier, thereby preventing the user from being charged
26 of a call made in an illegal use of the telephone.

27 On the other hand, the user is restricted so as to use only
28 one portable telephone under one contract, that is, in case
29 such the accounting information as the identification number
30 and phone number specific to the telephone is identical even

1 when the contractor is one and the same. Therefore, in case
2 a telephone is used separately for business activities and
3 for private activities, the user have had to make two
4 contracts. This has been a problem of the conventional
5 technique. In addition, in case the user wants to use a
6 PDA, a portable PC, etc. provided with communication
7 functions as a communication terminal other than the
8 portable telephone, the user have also had to make a
9 contract for each of those machines separately. And, in
10 order to solve such the problem, Published Unexamined Patent
11 Application No. 10-145523 discloses a technique for using a
12 card that stores a terminal identification number and a
13 technique for enabling a user to use a plurality of
14 communication terminals by sending/receiving a terminal
15 identification number through a communication port while
16 maintaining a condition that assigns one communication
17 terminal per one contract.

18 Problems to be solved by the invention

19 There is also a technique for protecting the true owner of a
20 portable telephone from illegal uses to be done when the
21 telephone itself is stolen or only the identification
22 information is used fraudulently so as to be set in another
23 portable telephone. In case a portable telephone is stolen
24 or lost, so that the telephone is away from the true owner,
25 the user, when knowing the fact, can get in contact with the
26 telephone company to stop the use so as to minimize the
27 damage. However, in case the identification number is
28 stolen and set in another telephone so as to make a copy
29 telephone while the owner of the telephone does not know it,
30 the damage might possibly be very great, since the user

1 cannot know the illegal uses of the copy telephone until the
2 user receives an account, which is usually received monthly.
3 Especially, in case a plurality of copy telephones are made,
4 the damage to be caused by illegal uses will become more
5 serious.

6 And, any of the conventional techniques described above does
7 not guarantee that the initial value of a scramble code is
8 never stolen even when it is set for each telephone; the
9 logic to scramble the code might also be analyzed. And,
10 even when the user is requested to input his/her password,
11 the conventional technique does not guarantee that the
12 password is never stolen. Updating, managing, and inputting
13 such a password are also troublesome.

14 Furthermore, in case it is enabled to use a plurality of
15 portable telephones or communication terminals selectively
16 under one contract, it means a higher possibility that the
17 telephones are copied illegally. And, any of the
18 conventional techniques described above cannot solve the
19 problem.

20 Summary of the invention

21 Under such circumstances, it is an object of the present
22 invention to provide a technique that can easily recognize a
23 fact that a password is stolen and set in another
24 communication terminal, which is then used as a copy
25 terminal. The technique is employed for such a
26 communication terminal as a portable telephone, etc. enabled
27 to communicate with another according to the identification

1 result of identification information and a password thereof.
2 It is another object of the present invention to provide a
3 technique that enables a plurality of communication
4 terminals to be used selectively under one contract while
5 effectively preventing illegal uses of a copy terminals
6 manufactured by a person other than the true owner.

7 Brief Description of the Drawings:

8 These and other aspects, features, and advantages of the
9 present invention will become apparent upon further
10 consideration of the following detailed description of the
11 invention when read in conjunction with the drawing figures,
12 in which:

13 Figure 1 is a schematic block diagram of a portable
14 telephone network in an embodiment of the present invention;

15 Figure 2 is a schematic block diagram of a portable
16 telephone in an embodiment of the present invention;

17 Figure 3 is a block diagram of a ROM 113;

18 Figure 4 is a block diagram of a configuration of a
19 non-volatile memory 117;

20 Figure 5 is a flowchart for describing the embodiment of the
21 present invention;

22 Figure 6 shows an embodiment of a contractor information
23 table;

1 Figure 7 shows another embodiment of the present invention;
2 and

3 Figure 8 is a flowchart for describing another embodiment of
4 the present invention.

5 Detailed Description of the Invention:

6 The first embodiment of the present invention is a
7 communication terminal provided with a non-volatile memory
8 that stores identification information and a password
9 thereof and enabled to communicate with a network after the
10 identification information and the password are collated.
11 The identification information and the password may be any
12 codes generated as such electronic information as
13 alphanumerics, symbols, etc. In this embodiment, a new
14 password different from the password having been sent to the
15 network at the start of each communication is generated
16 before the started communication is ended. Because such a
17 new password is generated during each communication, the
18 possibility that the password is stolen becomes lower than
19 when the user updates his/her password as needed. The
20 generated password is stored in the non-volatile memory, so
21 the user is not required to input the password by operating
22 keys each time the user begins a communication. The new
23 password is sent to the network before the communication is
24 ended. The password should preferably be sent together with
25 a communication termination code at the end of the
26 communication. Consequently, both of the communication
27 terminal and the network can hold the new password generated
28 during a communication at the end of the communication, so

1 that the network can enable the communication terminal to
2 start the next communication by collating the new password.

3 Because such a password is updated for each communication,
4 it is impossible that only a stolen password is used to
5 manufacture a copy terminal and the copy terminal is used
6 continuously while the true user does not know the fact.
7 Concretely, as long as the true user owns and uses his/her
8 normal communication terminal, the password is updated by
9 the true user for each communication. It is thus impossible
10 for any fraudulent user to use the copy terminal unless
11 he/she steals a new password at each communication. In case
12 the fraudulent user updates the password to use the normal
13 communication terminal at each communication just like the
14 true user, the communication is stopped when the normal
15 communication terminal is used because the normal
16 communication terminal cannot access the network with use of
17 the valid password that is recognized by the network at that
18 time. Therefore, the true user can know that his/her
19 password is used fraudulently. The communication terminal
20 may be any of radio and wire terminals or portable and
21 desk-top terminals.

22 The second embodiment of the present invention is a network
23 managed by a communication service provider. The network
24 enables each communication terminal to begin a communication
25 by comparing the information registered in its storage with
26 both identification information and password of the
27 communication terminal received at the start of the
28 communication. In addition, the network receives a new
29 password that is different from that received at the start
30 of the communication and stores the new password in the

1 storage before ending the communication. Consequently, both
2 of the communication terminal and the network hold the new
3 password, thereby the network compares the identification
4 information and the password sent from the communication
5 terminal at the start of the next communication with those
6 stored in the storage.

7 The third embodiment of the present invention is first and
8 second communication terminals used for communicating with
9 the network respectively. While only one communication
10 terminal is used under one contract, this embodiment can
11 prevent an illegal use of a copy terminal even when any
12 active one of the communication terminals is selected. Each
13 of the first and second communication terminals is provided
14 with a well-known function for enabling the information
15 stored in the non-volatile memory to be exchanged mutually.
16 The function may be realized by directly connecting a cable
17 to between the mutual communication ports or via the
18 network. In addition, it is also possible that the content
19 in one non-volatile memory is transferred to the other
20 non-volatile storage once, then the content is written in
21 the non-volatile memory of the other communication terminal.

22 Both identification information and password stored in the
23 first non-volatile memory of the first communication
24 terminal are transferred to and stored in the second
25 non-volatile memory of the second communication terminal.
26 And, the use of the first communication terminal is
27 inhibited, thereby the condition that only one terminal is
28 usable under one contract is secured. The password
29 transferred to the second non-volatile memory is a valid
30 password that is also held in the network at that time.

1 Hereinafter, the second communication terminal can
2 communicate with the network in the same way as that
3 described in the first embodiment. Still another embodiment
4 of the present invention is a communication terminal and a
5 network apparatus that can realize each of the embodiments
6 described above.

7 Preferred embodiment

8 Figure 1 shows a schematic block diagram of a portable
9 telephone network in an embodiment of the present invention.
10 A portable telephone network 25 supplied by a telephone
11 connection company includes base stations 15 and 17 for
12 sending/receiving and processing radio signals; a controller
13 19 for selecting a base station to which each portable
14 telephone is connected, controlling the connection of
15 telephones, accounting, etc.; a storage 21 including a
16 contractor information table; and a switchboard 23 for
17 connecting the network 25 to another communication network
18 27. In case a call is made from the portable telephone 11,
19 the call is connected to the network 25 via the base station
20 15 and further connected to another portable telephone 13
21 via the base station 17 under the control of the controller
22 19. Otherwise, the call is connected to another
23 communication network 27 via the switchboard 23.

24 Figure 2 shows a schematic block diagram of a portable
25 telephone 100 to which the present invention applies. An
26 antenna 101 is used to send/receive radio signals between
27 the base stations 15 and 17. The antenna 101 is connected
28 to a radio transmitter/receiver unit 102. The radio
29 transmitter/receiver unit 102 converts voice data to

1 communication data and vice versa, as well as
2 modulates/demodulates communication data and distinguishes
3 between voice data and control data. The radio
4 transmitter/receiver unit 102 is connected to a voice
5 processor 103 so that voice data is exchanged between them.
6 The voice processor 103 includes an encoder/decoder unit for
7 converting voice data to voice signals and vice versa. The
8 voice processor 103 is connected to a microphone 105 and a
9 speaker 107 that are combined so as to function as an
10 interface between the portable telephone 100 and the
11 operator with use of voices.

12 The control section 109 is mainly configured by a CPU. The
13 control section 109 controls the operation of the whole
14 portable telephone 100. The control section 109 is
15 connected to a communication interface 111. The
16 communication interface includes an RS232C serial interface
17 connector, which is used for data communication between a
18 telephone and an external device. The control section 109
19 is connected to the radio transmitter/receiver unit 102 and
20 the voice processor 103 respectively. The control section
21 109 sends/receives control data to/from the radio
22 transmitter/receiver unit 102 and controls those operations.

23 The control section 109 is connected to a ROM 113, a RAM
24 115, and a non-volatile memory 117 respectively. The ROM
25 113 stores an operation program required to operate the CPU
26 of the control section 109. The program in the ROM 113 is
27 kept as is when the power supply (not illustrated) of the
28 portable telephone 100 is turned off. The RAM 115 is used
29 to store data temporarily, which is to be processed by the
30 CPU. The data in the RAM 115 is erased when the power

1 supply of the portable telephone is turned off.

2 The non-volatile memory 117 should preferably be a flash
3 memory in which data can be written electrically. The data
4 in the memory 117 is kept as is when the power supply is
5 turned off. The non-volatile memory 117 stores the
6 identification number specific to a telephone, the telephone
7 number, and the password initial value written at a dealer
8 shop when the telephone is purchased. In addition, the
9 non-volatile memory 117 stores the telephone number, various
10 other set data of the telephone registered by the user who
11 purchased it. The information stored in the non-volatile
12 memory 117 can be sent/received to/from an external device
13 via the communication interface 111. The control section
14 109 is connected to a key pad 121 via a key sensor 119 and
15 further to a display 125 via a display control section 123.

16 The user uses the key pad 121 to input information required
17 to operate the telephone. The key sensor 119 generates a
18 key code according to an operated key and sends the key code
19 to the control section 109. The display control circuit 123
20 receives a signal denoting an operation state output from
21 the control section 109, a remote telephone number, etc. and
22 controls the display 125 so as to display the data
23 corresponding to the signal.

24 Next, a description will be made for a general operation of
25 the portable telephone 100 shown in Figure 2. When the user
26 purchases the telephone, the operation program is stored in
27 the ROM 113 as described above. In the non-volatile memory
28 117 are written initial values of set data items, the
29 identification number, and the user's phone number via the

1 communication interface 111. The owner, after purchasing
2 the telephone, operates the key pad 121 to write set data
3 items denoting specific party phone numbers and an easier
4 operation state for the user in the non-volatile memory 117.
5 In addition, the portable telephone 100 can be provided with
6 a removable recording medium (not illustrated). And, it is
7 possible to remove the recording medium after the
8 information stored in the non-volatile memory 117 is written
9 therein, then attach the medium to another portable
10 telephone so that the information is transferred to the
11 non-volatile memory of the object portable telephone.

12 Hereinafter, a description will be made on the assumption
13 that in case data is exchanged between two portable
14 telephones configured as shown in Figure 2 respectively via
15 base stations, the portable telephone 11 shown in Figure 1
16 makes a call and the portable telephone 13 receives the
17 call. In case the telephone 11 makes a call to the
18 telephone 13, the user inputs the phone number of the
19 telephone 13 directly from the key pad 121 of the telephone
20 11 or operates the key pad 121 to read the registered phone
21 number from the non-volatile memory 117 into the RAM 115.
22 Then, the user presses a call button on the key pad 121 to
23 make the control section 109 to start the calling. The
24 control section 109 calls both of the identification number
25 and individual phone number (of the telephone 11) from the
26 non-volatile memory 117 into the RAM 115 and sends them to
27 the radio transmitter/receiver unit 102 together with the
28 phone number of the telephone 13 and a communication start
29 code. The carrier is then modulated and those data items
30 are sent to the base station as modulated communication data
31 for calling from the antenna 101.

1 The base station has a contractor information table in its
2 storage 21. The contractor information table stores the
3 identification number, the phone number, the address, the
4 name, etc. of each telephone and information for identifying
5 its owner. Receiving communication data for calling from
6 the telephone 11, the base station 15 modulates and
7 processes the signal, then sends the data to the controller
8 19. The controller 19 collates both identification number
9 and phone number of the sending user with the data
10 registered in the contractor information table. And, in
11 case the call from the telephone is decided to be valid, the
12 controller transfers a calling signal to the phone number of
13 the telephone 13.

14 Receiving communication data for calling from the base
15 station via the antenna 101, the telephone 13 demodulates
16 the data in the radio transmitter/receiver unit 102 and
17 sends the demodulated data to the control section 109. The
18 control section 109, when recognizing that its telephone is
19 called, sends a calling signal to the voice processor so as
20 to generate a calling sound from the speaker 107. The owner
21 of the telephone 13 then operates the key pad 121 so as to
22 send a command to the control section 109 in response to the
23 calling sound. Receiving the command, the control section
24 109 controls the radio transmitter/receiver unit 102 and the
25 voice processor 103 so as to enable a communication to be
26 made via the microphone 105 and the speaker 107. The voice
27 signal inputted from the microphone 105 is encoded by the
28 voice processor 103 and converted to voice data. The voice
29 data is then sent to the radio transmitter/receiver unit
30 102, then converted to communication data and modulated.

1 After that, the modulated data is sent to the telephone 11
2 from the antenna 101 via the base station 17.

3 In case the receiving user starts communication, the control
4 signal is sent to the base station 17, thereby the
5 controller 19 begins accounting and the accounting
6 information is recorded in the contractor information table
7 of the sending user.

8 On the other hand, the telephone 11 receives voices and
9 control-related communication data from the base station 15.
10 The communication data received at the antenna 101, then
11 modulated is demodulated by the radio transmitter/receiver
12 unit 102. The control data is sent to the control section
13 109 and the voice data is sent to the voice processor 103.

14 Next, a description will be made for another embodiment in
15 which the present invention applies to the portable
16 telephone 100 shown in Figure 2 with reference to the
17 flowchart shown in Figure 5. Upon the application of the
18 present invention, the manufacturer of the telephone has
19 written the operation program 151 and a password updating
20 program 153 in the ROM 13 as shown in Figure 3. And, the
21 dealer company of the telephone has written the
22 identification number, the password, and the individual
23 phone number in the system area of the non-volatile memory
24 117 of the telephone as shown in Figure 4. In the user area
25 are written the phone number, set data items, etc. inputted
26 by the owner. At the sales time, the stored password is an
27 initial value. As to be described later in detail, the
28 password is updated each time a communication is ended
29 according to the present invention. In the storage of the

1 network 25 is stored a contractor information table as shown
2 in Figure 6.

3 The contractor information table stores the identification
4 number, phone number, the password, the accounting
5 information, etc. specific to each contractor. At this
6 time, the stored password is still an initial value. As to
7 be described later, the password is updated each time a
8 communication is ended according to the present invention.

9 Hereinafter, description for the general operations of the
10 telephone 100, which have already been described above, will
11 be omitted or described just simply. In block 201, the user
12 operates the key pad 121 so as to read the remote phone
13 number into the RAM 115. At this time, the operation
14 program 151 reads the identification number, the individual
15 phone number, and the password from the non-volatile memory
16 117 and stores them in the RAM 115 in block 203. Those data
17 items stored in the RAM 115 as described above are sent as
18 communication data for calling together with a communication
19 start code to the base station 15 of the network 25 via the
20 radio transmitter/receiver unit 102. The storage 21 of the
21 network 25 stores the contractor information table 300 as
22 shown in Figure 6. In block 205, the controller 19 that has
23 received the communication data for calling reads the
24 corresponding password from the contractor information table
25 300 according to the identification number and the phone
26 number.

27 The individual phone number may not be sent necessarily; it
28 can also be searched in the contractor information table
29 according to the identification number. In block 207, the

1 password received from the telephone 11 is compared with the
2 password read from the contractor information table by
3 referencing to the identification number. In block 209, it
4 is determined whether the comparison result is identical or
5 not. In case both passwords are identical, control goes to
6 block 211 so as to enable the communication to be started.
7 The controller 19 then begins counting of the communication
8 time for accounting. To end the communication in block 213,
9 the user presses the end button on the key pad 121 of the
10 portable telephone in block 215. Then, in block 217,
11 control of the control section 109 is passed to the password
12 updating program 153 in response to the pressed end button
13 of the portable telephone 11. The password updating program
14 153 then generates a new password, which is different from
15 the password (old password) stored in the non-volatile
16 memory 117 at that time. The password updating program 153
17 then overwrites the new password on the old password stored
18 in the non-volatile memory 117. This new password is used
19 for the next communication.

20 The password updating program may be any one that can
21 generate a password, which is different from the old
22 password. For example, the program may generate a new
23 password by performing an operation on an old password and a
24 predetermined constant. The program, however, should
25 preferably be able to generate a new password at random. In
26 case a portable telephone is provided with such the means
27 for generating a password at random, it will become
28 difficult for a fraudulent user to use the copy telephone
29 continuously without being found by the true user even when
30 the fraudulent user can steal the updating logic of the
31 password successfully. Such a random password may not

1 necessarily be generated only by software; it may be
2 generated by hardware.

3 In case a new password is generated in block 217, control of
4 the control section 109 is passed to the operation program
5 151. In block 219, therefore, the next password and the
6 communication termination code are sent to the base station
7 15. Although the next password is updated at the end of the
8 communication and sent to the network in this embodiment,
9 the present invention is not limited only to that
10 embodiment; a password, which is different from the password
11 used at the start of the communication, may be generated and
12 sent to the network before the end of the communication.

13 Receiving the termination code in block 221, the controller
14 19 ends the communication time counting for accounting and
15 updates the password (old password) in the contractor
16 information table shown in Figure 6 with the new password
17 received from the telephone 11 at the end of the
18 communication. The telephone 11 then overwrites the new
19 password on the old password stored in the password storing
20 area in the non-volatile memory 117 in block 223. After the
21 processings in blocks 221 and 223 are carried out, the new
22 password (used for the next communication) is stored in both
23 of the non-volatile memory 117 of the telephone 11 and in
24 the contractor information table 300 respectively.

25 In this embodiment, it will become apparent in the
26 description for blocks in and after 231, which is branched
27 from block 209 shown in Figure 5 that a true contractor can
28 find an illegal use of a copy telephone manufactured with
29 fraudulent use of an identification number and a password

1 that are stolen. As described in blocks 221 and 223,
2 disagreement between the password sent from the portable
3 telephone 11 in block 209 and the password stored in the
4 contractor information table 300 while the identification
5 number is the same is against the presumption that both of
6 the portable telephone 11 and the network must have the new
7 password updated at the end of the last communication with
8 respect to the identification number and the phone number.

9 Concretely, except for a technical write error to occur in
10 the non-volatile memory 117 and in the contractor
11 information table 300, the password sent from the telephone
12 11 this time is different from the password updated at the
13 end of the last communication. In case the last updated
14 password is stolen and it is set together with the
15 identification number and the phone number in a copy
16 telephone, which is used fraudulently, then the updated
17 password is stored in the contractor information table at
18 the end of the communication. And, in case the true
19 contractor attempts to make a call from the telephone 11
20 later, the password stored in the non-volatile memory 117 is
21 different from that stored in the contractor information
22 table. The controller 19 thus stops the communication in
23 block 231 even when the call is made by the true contractor
24 (user).

25 Furthermore, the controller 19 inhibits the use of the
26 portable telephone having the identification number
27 completely in block 233. Consequently, it is impossible to
28 use even the copy telephone in which the stolen password is
29 set after that. In block 235, the controller 19 notifies
30 the user of the fact that the portable telephone that is

1 making a call is disabled due to a detected illegal use of
2 the telephone according to the stolen password. Due to this
3 notification, the true owner of the portable telephone can
4 know the fraudulent use of the password, thereby getting in
5 contact with the communication service provider so as to
6 initialize the password and the identification number and
7 restart the use of the telephone.

8 Furthermore, it is also expected that the copy telephone
9 that has used a password fraudulently does not update the
10 password at the end of the communication and sends the old
11 password to the network. In such a case, the controller 19
12 can take a proper countermeasure; the controller stops the
13 communication in case the password received at the end of
14 the last communication does not agree to the password used
15 at the start of the communication. In case the controller
16 does not stop the communication, the old password used by
17 the true contractor for a communication is updated at the
18 end of the communication. Hereinafter, therefore, the
19 fraudulent user cannot use the telephone.

20 Another embodiment of the present invention is a system that
21 enables a plurality of portable telephones or a plurality of
22 such communication terminals as PDAs, lap-top PCs, etc.
23 provided with communication functions respectively to be
24 used under one contract. As described in the prior art
25 technique, only one communication terminal is usable under
26 one contract. Assume now that in Figure 7, the user
27 contracts for the portable telephone 100 described with
28 reference to Figures 2 and 5, so that the user is assigned
29 with an identification number, a phone number, and a
30 password. In this embodiment of the present invention, in

1 case one and the same user uses a portable PC 350 provided
2 with the same communication functions as those of the
3 portable telephone 100, there is no need for the user to
4 make another contract for the portable PC.

5 Next, a description will be made for a procedure that
6 changes a usable device from the portable telephone 100 to
7 the portable PC 350 selectively with reference to the
8 flowchart shown in Figure 8. The portable telephone 100 in
9 this embodiment is provided with a device change button on
10 the key pad 121. The portable PC 350 is a general personal
11 computer except for that the PC 350 is provided with the
12 same communication functions as those of the portable
13 telephone described with reference to the block diagram
14 shown in Figure 2. Detailed description for the PC 350 will
15 thus be omitted here. Concretely, the portable PC 350 is
16 provided with a keyboard; a display; and such a
17 communication port (equivalent to the communication
18 interface 111 shown in Figure 2) as the RS232C as external
19 devices and a CPU (equivalent to the control section 109
20 shown in Figure 2); a main memory (equivalent to the RAM 115
21 shown in Figure 2); an HDD (equivalent to the ROM 113 shown
22 in Figure 2); a flash memory (equivalent to the non-volatile
23 memory 117 shown in Figure 2); and an FDD as built-in
24 devices. The data processed in the CPU can be stored in the
25 HDD and/or transferred to an external device via the
26 communication port. The CPU or flash memory can store data
27 received from an external device.

28 At first, the RS232C communication interface of the portable
29 telephone is connected to the RS232C communication port of
30 the portable PC via a serial cable 351. In block 361, the

1 user presses the device change button of the portable
2 telephone. In block 363, the user transfers the
3 identification number, the phone number, the password, etc.
4 stored in the non-volatile memory 117 to the flash memory of
5 the portable PC 350 via the cable 351. Such data items as
6 the identification number, etc. are required to change
7 devices. At the same time, the user erases those data items
8 stored in the non-volatile memory 117 of the portable
9 telephone 100. The data required to change devices may be
10 transferred via a non-volatile recording medium without
11 using the communication port. The portable telephone 100,
12 when the identification number, etc. are erased, is disabled
13 (block 365).

14 On the other hand, the portable PC 350 receives the device
15 change data in block 367 and stores the data in the flash
16 memory of the portable PC 350 in block 369. After that, the
17 communication functions of the portable PC 350 become
18 available in block 371. In this state, the portable PC
19 communicates with the base station in the procedure
20 described with reference to Figure 5, thereby updating the
21 password at the end of the communication. In this
22 embodiment, therefore, even when the device change data of
23 the portable telephone 100 is stolen and transferred to
24 another communication terminal, the true contractor can
25 receive a notice of the illegal use and know the appearance
26 of a copy terminal when attempting a communication from the
27 portable PC 350, since the password is already updated due
28 to the access of the fraudulent user. And, even when the
29 fraudulent user avoids updating the password at the end of a
30 talking or communication, the communication service provider
31 stops the communication due to the use of the same password

1 as described above. Otherwise, the password is updated at
2 the end of the next communication by the true user, thereby
3 the fraudulent user cannot continue the use of the copy
4 terminal any longer.

5 Because a plurality of communication terminals are used
6 under one contract such way, this embodiment enables device
7 change data to be transferred and a plurality of portable
8 telephones to be used with a plurality of frequencies under
9 one contract in case, for example, a portable is used over
10 countries where different frequencies are used. The
11 embodiments described above are just examples and the
12 present invention should not be limited only to those
13 embodiment. The scope of the present invention, therefore,
14 is to be determined solely by the claims.

15 Advantages of the invention

16 According to the present invention, therefore, it is
17 possible to provide a communication method and a
18 communication terminal that enable a true contractor to
19 easily recognize an illegal use of a copy terminal
20 manufactured with a stolen password when beginning a
21 communication with a network provided with a storage that
22 stores the identification information and the password of
23 the contractor from a communication terminal provided with a
24 non-volatile memory that stores the identification
25 information and the password thereof. In addition, it is
26 possible to provide a communication method and a
27 communication terminal that can find and prevent an illegal
28 use of a copy terminal manufactured with a stolen password
29 easily even in case the true user is enabled to use a

1 plurality of communication terminals selectively under one
2 contract.

3 The present invention can be realized in hardware, software,
4 or a combination of hardware and software. A visualization
5 tool according to the present invention can be realized in a
6 centralized fashion in one computer system, or in a
7 distributed fashion where different elements are spread
8 across several interconnected computer systems. Any kind of
9 computer system - or other apparatus adapted for carrying
10 out the methods described herein - is suitable. A typical
11 combination of hardware and software could be a general
12 purpose computer system with a computer program that, when
13 being loaded and executed, controls the computer system such
14 that it carries out the methods described herein. The
15 present invention can also be embedded in a computer program
16 product, which comprises all the features enabling the
17 implementation of the methods described herein, and which -
18 when loaded in a computer system - is able to carry out
19 these methods.

20 Computer program means or computer program in the present
21 context include any expression, in any language, code or
22 notation, of a set of instructions intended to cause a
23 system having an information processing capability to
24 perform a particular function either directly or after
25 either or both of the following a) conversion to another
26 language, code or notation; b) reproduction in a different
27 material form.

28 It is noted that the foregoing has outlined some of the more

1 pertinent objects and embodiments of the present invention.
2 This invention may be used for many applications. Thus,
3 although the description is made for particular arrangements
4 and methods, the intent and concept of the invention is
5 suitable and applicable to other arrangements and
6 applications. It will be clear to those skilled in the art
7 that modifications to the disclosed embodiments can be
8 effected without departing from the spirit and scope of the
9 invention. The described embodiments ought to be construed
10 to be merely illustrative of some of the more prominent
11 features and applications of the invention. Other
12 beneficial results can be realized by applying the disclosed
13 invention in a different manner or modifying the invention
14 in ways known to those familiar with the art.